FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADEMICO DE INGENIERIA DE SISTEMAS DE INFORMACIÓN

TESIS

ANÁLISIS DEL NIVEL DE SEGURIDAD INFORMÁTICA DEL HOSPITAL CÉSAR GARAYAR GARCÍA IQUITOS-2023

PARA OBTAR EL TITÚLO PROFESIONAL

INGENIERO EN INFORMÁTICA Y SISTEMAS

INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTORES:

- **BACH. JUAN ARTURO RUIZ CÁCERES**
- **BACH. JORGE JUNIOR SÁNCHEZ RIOS**

ASESOR:

- **ING. RONALD PERCY MELCHOR INFANTES, Mtro.**

SAN JUAN BAUTISTA – MAYNAS

LORETO – PERÚ

2023

DEDICATORIA

"A Dios, quien ha sido mi guía y mi fortaleza en cada paso de mi camino. A mi familia, por su amor incondicional, apoyo constante y sacrificio para hacer posible este logro".

Bach. JUAN ARTURO RUIZ CÁCERES

"A Dios, a mis padres, a mi esposa y a todas las personas que me brindaron su apoyo y orientación, les agradezco de corazón por ser parte fundamental de este camino hacia el éxito".

Bach. JORGE JUNIOR SÁNCHEZ RIOS

AGRADECIMIENTO

"Queremos expresar nuestro sincero agradecimiento a las autoridades del Hospital Iquitos por habernos proporcionado las facilidades y la valiosa información que fueron fundamentales para el desarrollo de nuestra tesis.

A nuestro Asesor, cuya orientación experta y apoyo incondicional fueron cruciales en la elaboración y ejecución de este proyecto.

A la Universidad Científica del Perú, nuestra alma mater, por brindarnos el entorno académico propicio para crecer y aprender".

Bach. JUAN ARTURO RUIZ CÁCERES

Bach. JORGE JUNIOR SÁNCHEZ RIOS

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

UNIVERSIDAD CIENTÍFICA DEL PERÚ

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP

El presidente del Comité de Ética de la Universidad Científica del Perú - UCP

Hace constar que:

La Tesis titulada:

"ANÁLISIS DEL NIVEL DE SEGURIDAD INFORMÁTICA DEL HOSPITALCÉSAR GARAYAR GARCÍA IQUITOS-2023"

De los alumnos: **JUAN ARTURO RUIZ CÁCERES Y JORGE JUNIOR SÁNCHEZ RIOS,** de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **14% de similitud**.

Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 09 de enero del 2024.

Mgr. Arq. Jorge L. Tapullima Flores
Presidente del Comité de Ética – UCP

CJRA/ri-a
13-2024

Resultados_UCP_INGENIERIADESISTEMAS_2023_TESIS_JUNI...

INFORME DE ORIGINALIDAD

14%	13%	2%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unapiquitos.edu.pe Fuente de Internet	1%
2	repositorio.uladech.edu.pe Fuente de Internet	1%
3	idoc.pub Fuente de Internet	1%
4	www.coursehero.com Fuente de Internet	1%
5	risti.xyz Fuente de Internet	1%
6	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1%
7	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	<1%
8	repositorio.ucv.edu.pe Fuente de Internet	<1%
9	cybertesis.unmsm.edu.pe Fuente de Internet	

turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Juan Arturo Ruiz Cáceres
Título del ejercicio:	Quick Submit
Título de la entrega:	Resultados_UCP_INGENIERIADESISTEMAS_2023_TESIS_JUNI...
Nombre del archivo:	UCP_INGENIERIADESISTEMAS_2023_TESIS_JUNIORSANCHEZ_...
Tamaño del archivo:	812.03K
Total páginas:	47
Total de palabras:	9,690
Total de caracteres:	57,568
Fecha de entrega:	14-dic.-2023 11:57a. m. (UTC-0500)
Identificador de la entre...	2259028046

Universidad Científica del Perú - UCP

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADEMICO DE INGENIERIA DE SISTEMAS DE INFORMACIÓN

INFORME FINAL DE TESIS

ANÁLISIS DEL NIVEL DE SEGURIDAD INFORMÁTICA DEL HOSPITAL CÉSAR GARAYAR GARCÍA IQUITOS-2023

PARA OBTAR EL TITÚLO PROFESIONAL

INGENIERO EN INFORMÁTICA Y SISTEMAS

INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTORES:

- BACH. JUAN ARTURO RUIZ CÁCERES
- BACH. JORGE JUNIOR SÁNCHEZ RIOS

ASESOR:

- ING. RONALD PERCY MELCHOR INFANTES, Mtro.

SAN JUAN BAUTISTA – MAYNAS

LORETO – PERÚ

2023

ACTA DE SUSTENTACIÓN

FACULTAD DE CIENCIAS E INGENIERÍA

UNIVERSIDAD CIENTÍFICA DEL PERÚ

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N° 363-2023-UCP-FCEI del 18 de mayo del 2023, la Facultad de Ciencias e Ingeniería de la Universidad Científica del Perú - UCP designa como Jurado Evaluador de la tesis a los señores:

- Ing. Jimmy Max Ramírez Villacorta, Mtro. — Presidente
- Ing. Ángel Alberto Marthans Ruíz, Mgr. — Miembro
- Ing. Tonny Eduardo Bardales Lozano, Mgr. — Miembro

Como Asesor de la Tesis, Ing. Ronald Percy Melchor Infantes, Mgr.

En la ciudad de Iquitos, siendo las **10:00 am** del día **09 de mayo de 2024,** supervisado por la Secretaria Académica del Programa de Ingeniería de Sistemas de Información de la Facultad de Ciencias e Ingeniería de la Universidad Científica del Perú, se constituyó el Jurado para escuchar la sustentación y defensa de la Tesis: ***ANÁLISIS DEL NIVEL DE SEGURIDAD INFORMÁTICA DEL HOSPITAL CESAR GARAYAR GARCIA IQUITOS 2023,***

Presentado por las sustentantes

- **SANCHEZ RÍOS JORGE JUNIOR**
- **RUIZ CACERES JUAN ARTURO**

Como requisito para optar el título Profesional de:

- **INGENIERO DE SISTEMAS DE INFORMACIÓN**
- **INGENIERO INFORMÁTICO Y DE SISTEMAS**

Luego de escuchar la sustentación y formuladas las preguntas las que fueron: ABSUELTAS

El Jurado después de la deliberación en privado llegó a la siguiente conclusión:
Que la sustentación es APROBADO POR UNANIMIDAD

En fe de lo cual los miembros del Jurado firman el acta.

Ing. Jimmy Max Ramírez Villacorta, Mtro.
Presidente

Ing. Ángel Alberto Marthans Ruíz, Mgr.
Miembro

Ing. Tonny Eduardo Bardales Lozano, Mgr
Miembro

APROBACIÓN

HOJA DE APROBACIÓN

PROGRAMA ACADÉMICO DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS e INGENIERÍA DE SISTEMAS INFORMACIÓN
TESISTAS: RUIZ CACERES JUAN ARTURO Y SANCHEZ RÍOS JORGE JUNIOR

Tesis sustentada en acto publico el 09 de mayo de 2024, a las 10:00 am en las instalaciones de la UNIVERSIDAD CIENTÍFICA DEL PERÚ.

ING. JIMMY MAX RAMÍREZ VILLACORTA, MTRO..
PRESIDENTE DE JURADO

ING. ÁNGEL ALBERTO MARTHANS RUÍZ, MGR.
.MIEMBRO DE JURADO

ING. TONNY EDUARDO BARDALES LOZANO, MGR.
MIEMBRO DE JURADO

ING. RONALD PERCY MELCHOR INFANTES, MGR
ASESOR

INDICE DEL CONTENIDO

ÍNDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

La investigación realizada en el Hospital César Garayar García en Iquitos en el año 2023 se enmarca en un enfoque descriptivo y evaluativo. Se ha utilizado el enfoque descriptivo para comprender y describir el estado actual de la seguridad informática en el hospital, y el enfoque evaluativo se ha aplicado para analizar y evaluar el nivel de seguridad informática existente en la institución. Para llevar a cabo esta investigación, se recopilaron datos, se realizaron evaluaciones de vulnerabilidades y se analizaron las políticas y prácticas de seguridad, el diseño de la investigación se clasifica como un estudio de caso, ya que se centra en un caso específico, que es el Hospital César Garayar García en Iquitos. Se ha realizado un análisis detallado y profundo de la entidad, centrándose en la evaluación de la seguridad informática en el hospital, la población de estudio incluyó todos los sistemas informáticos, dispositivos, políticas de seguridad y personal relacionado con la seguridad informática en el Hospital César Garayar García en Iquitos en el año 2023. La muestra se compuso de una variedad de activos de hardware y software, así como personal relacionado con la seguridad informática, las técnicas de recolección de datos utilizadas incluyeron observación, entrevistas y auditorías de seguridad. Los instrumentos de recolección de datos consistieron en fichas de observación, cuestionarios y una matriz de riesgo para evaluar los activos de información. Se detalla el procedimiento de recolección de datos para cada técnica, el procesamiento y análisis de datos se realizaron utilizando software estadístico SPSS Versión 22, y los resultados se presentaron en forma de cuadros y gráficos estadísticos, los resultados se dividieron en varias dimensiones y se discutieron en detalle, Evaluación del Hardware: Se evaluó el estado actual de los activos de hardware del hospital, y la mayoría se encontró en buen estado, aunque algunos equipos de escritorio y otros elementos se clasificaron como regulares, necesidades de Hardware: Se identificaron equipos de hardware necesarios para mejorar la infraestructura tecnológica y la comunicación en el hospital, como un firewall, un switch Core y servidores de telefonía IP, posibles Vulnerabilidades del Software: Se señalaron posibles vulnerabilidades en los sistemas informáticos utilizados en el hospital, como el acceso no autorizado y vulnerabilidades en el software, Matriz de Riesgo de Activos de Información: Se elaboró una matriz de riesgo que clasifica

los activos de información en función de su importancia, vulnerabilidad y riesgo, resaltando la necesidad de proteger activos críticos, se concluyó que la evaluación del hardware muestra que la mayoría de los activos de hardware están en buen estado, pero se deben abordar los elementos clasificados como regulares, se identificaron las necesidades de hardware necesarias para mejorar la infraestructura tecnológica del hospital, se destacó la importancia de identificar y mitigar posibles vulnerabilidades en los sistemas informáticos, la matriz de riesgo subrayó la importancia de priorizar la seguridad de activos críticos y tomar medidas adecuadas para protegerlos, se formularon recomendaciones específicas, como implementar un programa de mantenimiento preventivo y correctivo, adquirir activos de hardware necesarios, fortalecer la seguridad de software y priorizar la seguridad de activos críticos, estas recomendaciones buscan mejorar la seguridad informática en el Hospital César Garayar García y garantizar la protección de datos sensibles y la eficiencia operativa en la institución.

Palabras claves: Seguridad, informática, hospital.

ABSTRACT

The research conducted at the César Garayar García Hospital in Iquitos in the year 2023 is framed within a descriptive and evaluative approach. The descriptive approach was used to understand and describe the current state of information security at the hospital, and the evaluative approach was applied to analyze and evaluate the existing level of information security within the institution. To carry out this research, data was collected, vulnerability assessments were conducted, and security policies and practices were analyzed, the research design is categorized as a case study, as it focuses on a specific case, which is the César Garayar García Hospital in Iquitos. A detailed and in-depth analysis of the entity has been conducted, with a focus on evaluating information security at the hospital, the study population included all computer systems, devices, security policies, and personnel related to information security at the César Garayar García Hospital in Iquitos in the year 2023. The sample was composed of a variety of hardware and software assets, as well as personnel related to information security, data collection techniques used included observation, interviews, and security audits. Data collection instruments consisted of observation sheets, questionnaires, and a risk matrix to assess information assets. The data collection procedure for each technique is detailed, data processing and analysis were carried out using statistical software SPSS Version 22, and the results were presented in the form of statistical tables and graphs, the results were divided into several dimensions and discussed in detail: Hardware Assessment: The current state of the hospital's hardware assets was evaluated, and the majority were found to be in good condition, although some desktop computers and other elements were classified as regular, Hardware Needs: Necessary hardware equipment was identified to improve the hospital's technological infrastructure and communication, such as a firewall, a Core switch, and IP telephone servers, Potential Software Vulnerabilities: Potential vulnerabilities in the computer systems used at the hospital were identified, such as unauthorized access and software vulnerabilities, Information Asset Risk Matrix: A risk matrix was developed to classify information assets based on their importance, vulnerability, and risk, emphasizing the need to protect critical assets, it was concluded that the hardware assessment shows that most hardware assets are in good condition, but the items classified as regular need to be addressed. The identified hardware needs are essential to enhance the hospital's technological

infrastructure, The importance of identifying and mitigating potential vulnerabilities in computer systems was highlighted. The risk matrix emphasized the need to prioritize the security of critical assets and take appropriate measures to protect them, specific recommendations were formulated, such as implementing a preventive and corrective maintenance program, acquiring necessary hardware assets, strengthening software security, and prioritizing the security of critical assets. These recommendations aim to improve information security at the César Garayar García Hospital and ensure the protection of sensitive data and operational efficiency within the institution.

Keywords: Security, information technology, hospital.

CAPÍTULO I: MARCO TEÓRICO

1.1. Antecedentes de Estudio

Salazar, Juan & Campoverde, Milton (2022), en su artículo científico hacen mención que, en el entorno actual, la constante evolución de la integración de las tecnologías de la información y la comunicación en las instituciones de salud del sector público es innegable. Esta evolución se refleja en el uso de diversas infraestructuras informáticas para hacer frente a desafíos significativos relacionados con la gestión de sistemas de salud. A medida que estas tecnologías han crecido y se han fusionado en las operaciones de estas instituciones, se ha manifestado una preocupante tendencia: el incremento de actividades delictivas en línea por parte de actores de ciberdelincuencia. Estos agentes maliciosos buscan activamente debilidades en los sistemas de información, con un enfoque en el recurso más valioso de las organizaciones: la información, ante este panorama, se hace indispensable la adopción de medidas destinadas a controlar las vulnerabilidades y a disminuir el riesgo de vulneraciones de la seguridad de la información. Estos esfuerzos deben centrarse en preservar la confidencialidad, la integridad y la disponibilidad de los datos en un entorno donde la información médica es crítica, en este contexto, el presente estudio se enfoca en la identificación y análisis de problemas de seguridad informática en el Hospital de Especialidades "José Carrasco Arteaga," ubicado en la ciudad de Cuenca, Ecuador. Para llevar a cabo esta investigación, se ha empleado una metodología que involucra técnicas de Hacking Ético, aplicadas de manera ética y legal, en las estaciones de trabajo y las redes de esta institución de salud. Los resultados de esta investigación han revelado la presencia de niveles significativos de vulnerabilidades, la mayoría de las cuales se pueden resolver a través de medidas de mitigación o soluciones proporcionadas por los fabricantes de sistemas.

Arismendi, Jonathan, Et Al. (2018), En el marco de esta tesis, se lleva a cabo un proyecto aplicado en una institución de salud de carácter público de segundo nivel de complejidad, ubicada en el municipio de Dosquebradas, Departamento de Risaralda. Dicha institución de salud gestiona información de gran sensibilidad, que incluye el registro de historias clínicas de todos los pacientes atendidos, así como datos administrativos y financieros de relevancia. Conscientes de la importancia de salvaguardar esta información, se emprendió un análisis detallado y la identificación de los riesgos a los que está expuesta la infraestructura de la red de datos de la institución, con el objetivo de identificar posibles amenazas que puedan comprometer la seguridad informática y la integridad de los datos de la institución, el proceso de recopilación de información se inició con entrevistas al personal encargado de la gestión de las redes de datos de la institución. Estas conversaciones permitieron identificar aspectos cruciales que planteaban desafíos en términos de seguridad informática. A continuación, se realizó una inspección física exhaustiva en cada una de las sedes que conforman la entidad, con especial énfasis en la revisión y la identificación visual de todos los componentes que forman parte de la infraestructura de la red de datos, posteriormente, se llevaron a cabo pruebas de penetración, empleando herramientas basadas en software libre, para evaluar la resistencia de la red de datos ante posibles ataques cibernéticos. Todos los hallazgos obtenidos a lo largo de este proceso fueron recopilados y se plasmaron en un documento final, basándose en los resultados de esta evaluación, se propuso un conjunto de medidas de mitigación como parte de un plan de mejora. Estas propuestas se entregaron a la coordinación del área de tecnología de la institución con el propósito de que fueran evaluadas y se llevaran a cabo las acciones necesarias, adaptadas a la capacidad de la empresa, con el fin de fortalecer la seguridad informática y proteger la integridad de los datos de la institución. Esta investigación proporciona una base sólida para el desarrollo del proyecto aplicado y destaca la importancia de garantizar la seguridad de la información en el entorno de la salud.

Cutin, Alipio (2020), El presente trabajo de investigación se enmarca en el contexto de la Municipalidad Distrital de Canchaque, donde se aborda la cuestión de los sistemas de gestión de calidad y seguridad de la información. Se enfoca particularmente en el área de secretaría y fotocopiado, así como en las cuatro oficinas que están equipadas con computadoras. Dentro de este marco, se ha identificado una problemática significativa relacionada con los procesos de modificación de información, los cuales involucran tanto a los trabajadores de la institución como a los ciudadanos que interactúan con ella, uno de los factores clave que ha motivado esta investigación es el alto riesgo que presenta la gestión de la información en esta municipalidad. La rotación constante de empleados agrega una capa adicional de complejidad y vulnerabilidad a los procesos de modificación de datos. Además, se ha identificado una seria preocupación con respecto a la seguridad de la información, especialmente para los empleados que utilizan computadoras de escritorio en su trabajo diario. La posibilidad de robo de datos por parte de terceros o incluso errores cometidos por los propios empleados al manipular información importante, son cuestiones que generan inquietud en la institución, en respuesta a estas problemáticas, el objetivo principal de esta investigación ha sido el análisis y diseño de un plan de seguridad informática específicamente orientado a la Municipalidad Distrital de Canchaque. Este plan tiene como propósito fundamental mejorar el control y la protección de datos e información sensible, abordando de manera efectiva los riesgos identificados, para llevar a cabo esta investigación, se adoptó un enfoque cuantitativo dentro del marco de la investigación descriptiva, con un diseño no experimental de corte transversal. La población de estudio se conformó por 10 trabajadores de la municipalidad, seleccionados mediante un método de conveniencia. Para la recolección de datos, se emplearon técnicas de encuesta y observación, lo que permitió obtener una visión detallada de las percepciones y prácticas de los trabajadores en relación con el sistema actual, como resultado de este estudio, se logró el diseño de un plan de seguridad informática que obtuvo una notable aceptación, alcanzando un nivel del 100.00%. Esta investigación culminó de manera exitosa, cumpliendo con el objetivo general planteado y brindando una sólida base para la implementación de medidas que fortalezcan la seguridad de la información en la Municipalidad Distrital de Canchaque.

Chávez, Eduard; Dávila, Willy (2022), En el marco de la presente tesis titulada "Evaluación del Nivel de Seguridad de la Información en el Hospital III Iquitos de Essalud Loreto – 2022," se ha realizado un exhaustivo examen de las vulnerabilidades y amenazas que afectan a la Unidad de Soporte Informático de dicho hospital. La evaluación se ha basado en una metodología de enfoque cuantitativo, que se ha centrado en describir los criterios técnicos que determinan el funcionamiento y la calidad de los servicios proporcionados por esta unidad, tanto a los usuarios internos como a los externos, este análisis se ha fundamentado en los principios fundamentales de la seguridad de la información, a saber, la Disponibilidad, la Integridad y la Confidencialidad. El objetivo general de este trabajo de investigación ha sido evaluar los niveles de seguridad de la información en el Hospital III Iquitos de Essalud. Como resultado de esta evaluación, se ha identificado la carencia de protocolos y mecanismos esenciales para garantizar la precisión de la información en su procesamiento, transporte y almacenamiento. Además, se ha constatado la ausencia de criterios seguros y fiables que faciliten un acceso oportuno a los sistemas informáticos. Por último, se ha observado la falta de criterios y mecanismos de seguridad para asegurar la accesibilidad y el control de ingreso autorizado a los sistemas informáticos por parte de aquellas personas que cuentan con las credenciales o la autorización necesaria para procesar la información, según lo definido por el área usuaria, estas conclusiones subrayan la imperante necesidad de implementar un Sistema de Gestión de Seguridad de la Información en el entorno del hospital, en este contexto, se recomienda específicamente la adopción de la norma "NTP ISO/IEC 27001:2014". Estos hallazgos constituyen un sólido fundamento para la investigación que se llevará a cabo en el marco de esta tesis, y apuntan a la importancia crítica de abordar y mejorar la seguridad de la información en el contexto hospitalario.

Cordero, José, Et Al. (2016), El presente trabajo de tesis documenta una serie de análisis de riesgos que se han identificado en la Empresa Social del Estado (E.S.E.) Hospital San Bartolomé, ubicado en el municipio de Capitanejo. Estos riesgos se han manifestado como consecuencia de un cambio en la infraestructura tecnológica y la falta de implementación de políticas de seguridad adecuadas en la administración de tres servidores fundamentales. Estos servidores almacenan información crítica relacionada con todos los procesos administrativos, operativos y financieros de la empresa, la necesidad de abordar este estudio surge de la importancia de garantizar la confidencialidad, integridad y disponibilidad de la información en la institución de salud. Como resultado de este análisis, se plantea la formulación de recomendaciones en materia de seguridad informática. El objetivo es optimizar la fortaleza de los procesos, asegurando que la información sensible se mantenga protegida de amenazas y riesgos potenciales, el producto final de este estudio consistirá en una serie de recomendaciones y alternativas concretas para abordar y mitigar los riesgos identificados en los procesos, procedimientos y recursos que albergan información crítica para el hospital. Estas recomendaciones permitirán la creación de mecanismos, estrategias y una cultura de seguridad en el personal de la institución. Se contempla la posibilidad de llevar a cabo procesos de capacitación y concienciación del personal para promover el uso adecuado de los recursos tecnológicos y fortalecer la seguridad de la información. El propósito final es garantizar la integridad y la confidencialidad de los datos, así como la disponibilidad de los recursos tecnológicos en el entorno hospitalario.

1.2. Bases Teóricas

La seguridad informática, según Morales (2022), se define como el conjunto de medidas técnicas, organizativas y legales destinadas a proteger los sistemas informáticos, redes y dispositivos contra accesos no autorizados, modificaciones, divulgación, destrucción o interrupción de los servicios que brindan. Su principal objetivo es garantizar la integridad, confidencialidad y disponibilidad de los datos, además de prevenir interrupciones y fallos en los sistemas informáticos. La creciente complejidad de los sistemas y las

amenazas informáticas sofisticadas han subrayado la importancia de la seguridad informática en la actualidad.

La seguridad informática se ha convertido en un tema de interés público en los últimos años, con términos como "clave de usuario", "contraseña", "fraude informático" y "hacker" siendo comunes tanto para expertos como para usuarios comunes. En la actualidad, contar con sólidos conocimientos en este campo es esencial para evitar poner en riesgo la información, el equipo y la integridad del usuario.

Gómez (2006) la define como cualquier medida que previene la ejecución de operaciones no autorizadas en sistemas o redes informáticas que puedan causar daños a la información, el equipo o el software.

Kissel (2012) la relaciona con la protección de la información y los sistemas de información de accesos no autorizados, involucrando tres elementos fundamentales: información, software y hardware.

Para garantizar la seguridad de los datos, es fundamental cumplir con tres componentes esenciales: integridad, disponibilidad y confidencialidad.

Figura 1: Objetivos de la seguridad de la información

Fuente: https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/

En cuanto a los tipos de seguridad informática, se pueden destacar:

Seguridad física: Enfocada en la protección de dispositivos físicos y el acceso a ellos, incluyendo medidas como el control de acceso a instalaciones, el uso de cerraduras y la protección de equipos de cómputo.

Seguridad lógica: Se centra en la protección del software y los datos, involucrando medidas como contraseñas, autenticación de usuarios, gestión de permisos, firewalls y cifrado de datos.

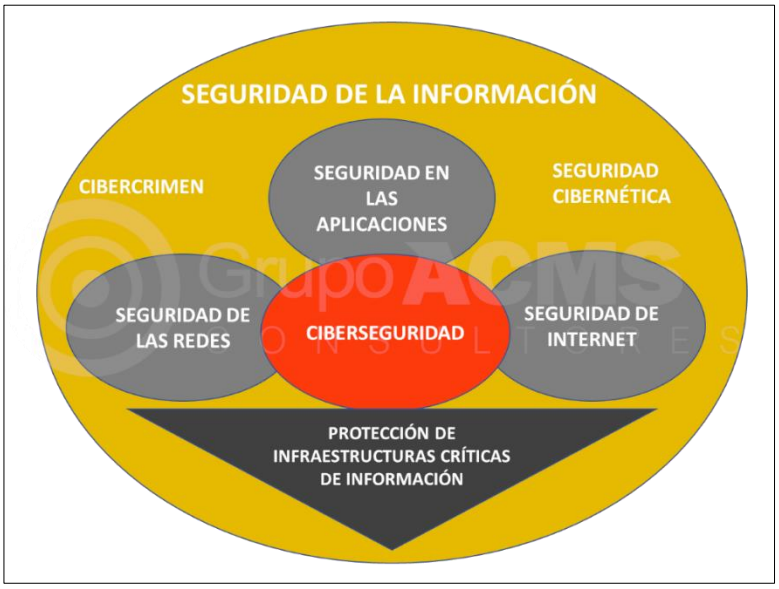
Seguridad de red: Orientada a proteger las redes y la información transmitida a través de ellas, utilizando firewalls, autenticación de usuarios, VPN, monitoreo del tráfico y prevención de ataques DoS.

Seguridad de la información: Su objetivo es la protección de la información en sistemas o redes, a través de políticas de seguridad, control de acceso y prevención de pérdida de datos.

Seguridad de aplicaciones: Dirigida a proteger las aplicaciones de software utilizadas en sistemas o redes, mediante prácticas de codificación segura, gestión de permisos y prevención de vulnerabilidades.

Estos tipos de seguridad informática son esenciales para proteger los sistemas y redes de posibles amenazas. Los objetivos de la seguridad informática, por su parte, incluyen la confidencialidad, integridad, disponibilidad, autenticación, autorización, responsabilidad, no repudio y protección física de hardware y dispositivos. Estos objetivos buscan garantizar la protección de la información, los sistemas y las redes, y asegurar que los usuarios autorizados puedan acceder a la información cuando sea necesario. La responsabilidad y la no repudio también son importantes para rastrear y responsabilizar a los usuarios por sus acciones en el sistema, mientras que la seguridad física protege el hardware y los dispositivos críticos.

Figura 2: Tipos de seguridad de la información



Fuente: https://www.grupoacms.com/seguridad-informacion.php

Una célebre cita que ha ganado renombre en el ámbito de la seguridad proviene de Eugene Spafford, destacado profesor de ciencias informáticas en la Universidad Purdue de Indiana, EE. UU. Spafford expresó que "el único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él." Hablar de seguridad informática en términos absolutos resulta una empresa imposible, lo cual nos lleva a enfocarnos en la fiabilidad del sistema, que, en esencia, representa una perspectiva más realista.

La fiabilidad, en este contexto, se define como la probabilidad de que un sistema se comporte de acuerdo a las expectativas preestablecidas.

En términos generales, un sistema puede considerarse seguro y fiable si podemos garantizar tres elementos fundamentales:

Confidencialidad: Garantizar que el acceso a la información ocurra únicamente a través de autorización y de manera controlada.

Integridad: Asegurar que la modificación de la información solo sea posible con autorización, preservando su integridad original.

Disponibilidad: Mantener la información del sistema accesible mediante autorización, evitando interrupciones no autorizadas.

Estos son los pilares clave para evaluar y garantizar la seguridad y fiabilidad de los sistemas informáticos, reconociendo que la seguridad absoluta es una utopía y que la fiabilidad es un objetivo más realista en la práctica.

Además, existen diversos tipos de seguridad informática empleados para salvaguardar los sistemas y redes de posibles amenazas. A continuación, se detallan algunos de los tipos más comunes:

Seguridad Física: Se refiere a la protección de los dispositivos físicos y la gestión del acceso a ellos. Esto incluye medidas como la restricción de acceso a instalaciones, el uso de cerraduras, el control de ingreso a áreas críticas y la seguridad de los equipos de cómputo.

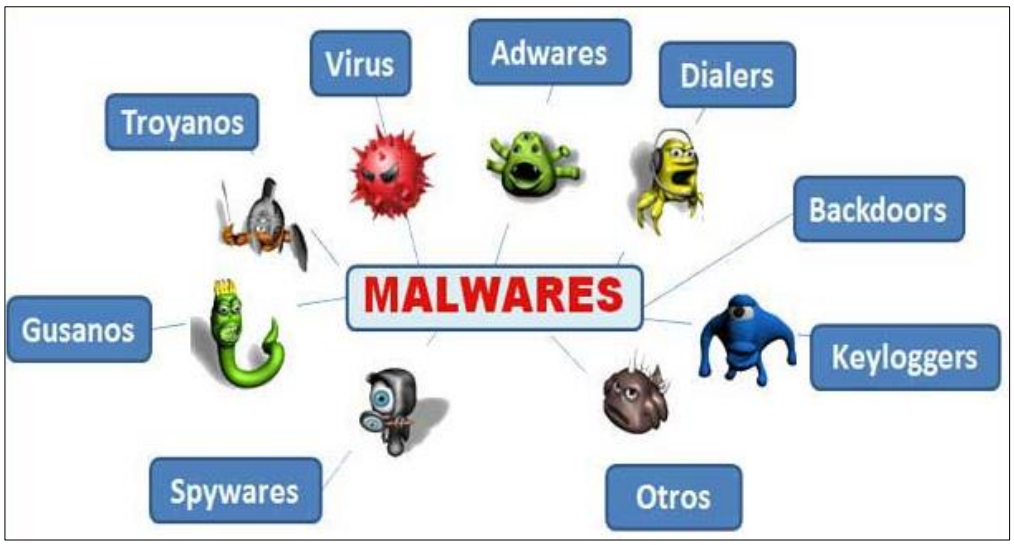
Figura 3: Seguridad física de la información

Fuente: Ergo

Seguridad Lógica: Esta categoría se enfoca en la protección del software y los datos que residen en un sistema o red. Comprende elementos como el uso de

contraseñas, la autenticación de usuarios, la gestión de permisos, la implementación de firewalls y el cifrado de datos.

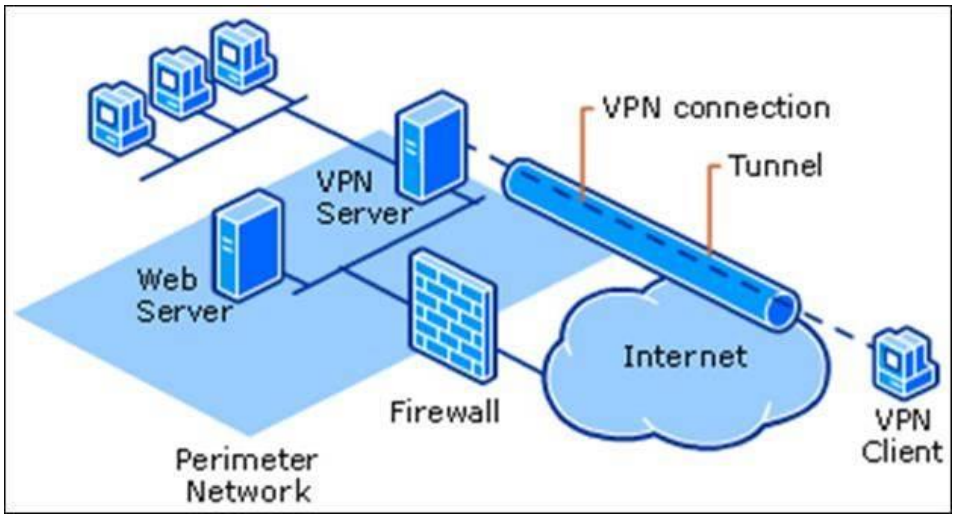
Figura 4: Seguridad lógica de la información



Fuente: https://soniaespitia.github.io/LecturasSeguridadInformatica/

Seguridad de Red: Su propósito principal es resguardar las redes informáticas y los datos que fluyen a través de ellas. Incluye la implementación de firewalls, autenticación de usuarios, configuración de VPNs (redes privadas virtuales), supervisión del tráfico de red y prevención de ataques de denegación de servicio (DoS).

Figura 5: Seguridad de red



Fuente: https://www.lisot.com/seguridad-en-una-red-de-datos/

Seguridad de la Información: Se centra en la protección de la información almacenada en un sistema o red. Implica la definición y aplicación de políticas de seguridad, la gestión del acceso a la información y la prevención de pérdida de datos.

Seguridad de Aplicaciones: Esta área se dedica a proteger las aplicaciones de software utilizadas en un sistema o red. Incluye la implementación de prácticas de codificación segura, la administración de permisos y la prevención de vulnerabilidades de seguridad.

Es fundamental destacar que este campo experimenta una constante evolución con la aparición de nuevas amenazas y técnicas. Por lo tanto, resulta esencial mantenerse actualizado respecto a las tendencias y mejores prácticas en seguridad informática para proteger eficazmente los sistemas y redes.
Políticas de seguridad:

De acuerdo con las afirmaciones de Laudon, K. C. y Laudon, J. P. (2012), así como las de García Pierrat, G. y Vidal Ledo, M. J. (2016), para asegurar la protección de los activos informáticos frente a los riesgos identificados, es imperativo desarrollar una política de seguridad. Dicha política posibilita la utilización eficiente y segura de las tecnologías de la información y las comunicaciones al establecer las directrices sobre su empleo. Las políticas de seguridad establecen normativas para el personal involucrado en el sistema informático, definen el uso adecuado de los recursos informáticos, regulan el acceso a los mismos, gestionan la identidad de los usuarios, determinan la política de privacidad de la empresa, establecen la responsabilidad de los usuarios y regulan el uso de equipos y redes corporativas para fines personales.

De acuerdo con García Pierrat, G. y Vidal Ledo, M. J. (2016), las políticas de seguridad representan la estrategia global de la empresa, mientras que las medidas y procedimientos constituyen los pasos específicos necesarios para alcanzar la seguridad informática. Es fundamental que una política de seguridad eficaz pueda ser implementada a través de estas medidas y procedimientos.

Medidas de seguridad:

A partir de la identificación de posibles eventos que puedan impactar a la empresa, las medidas y procedimientos de seguridad definen las acciones requeridas, los recursos necesarios y las responsabilidades pertinentes. No existe una combinación de controles universalmente óptima, ya que cada empresa es única y, por lo tanto, se necesita realizar un análisis de riesgos para identificar los activos más susceptibles en cada caso particular. En contraste con las políticas de seguridad generales, las medidas y procedimientos son específicos y se aplican de manera personalizada según las necesidades particulares de cada área (García Pierrat, G. y Vidal Ledo, M. J., 2016).

Conforme a la explicación de Saroka, R. H. (2002), las medidas de seguridad se pueden clasificar en tres categorías distintas:

Medidas preventivas: Orientadas a reducir la probabilidad de que las amenazas se materialicen mediante acciones destinadas a prevenir o minimizar su impacto.

Medidas de detección: Diseñadas para mitigar los efectos de las amenazas una vez que se han concretado y para identificar oportunamente los eventos que puedan surgir.

Medidas correctivas: Dirigidas a restaurar la capacidad de operación normal resolviendo los problemas que hayan surgido.

1.3. Definición de Términos Básicos:

Firewall: Un firewall es una barrera de seguridad que protege una red o sistema de amenazas al controlar el tráfico de red entrante y saliente.

Malware: Es un término genérico que engloba software malicioso como virus, gusanos, troyanos y spyware que se utiliza para dañar o robar información.

Antivirus: Es un programa diseñado para detectar, prevenir y eliminar el malware de un sistema.

Cifrado: El cifrado es el proceso de convertir datos en un código para proteger su confidencialidad.

Phishing: El phishing es una técnica en la que los ciberdelincuentes intentan engañar a las personas para que revelen información confidencial, como contraseñas y números de tarjetas de crédito.

Ingeniería social: La ingeniería social implica manipular a las personas para que divulguen información confidencial o realicen acciones específicas.

Autenticación de dos factores (2FA): La 2FA es un método de seguridad que requiere dos formas diferentes de autenticación antes de permitir el acceso a una cuenta o sistema.

Backup: Una copia de seguridad es una réplica de los datos importantes que se utiliza para recuperar la información en caso de pérdida o daño.

Actualización de software: Mantener el software actualizado es esencial para parchear vulnerabilidades y mejorar la seguridad.

Política de contraseñas: Una política de contraseñas establece las reglas para la creación y gestión de contraseñas seguras.

Auditoría de seguridad: La auditoría de seguridad implica la revisión y evaluación de un sistema o red para identificar vulnerabilidades y riesgos.

Control de acceso: El control de acceso consiste en regular quién tiene permiso para acceder a sistemas, aplicaciones o datos.

VPN (Red Privada Virtual): Una VPN crea una conexión segura a través de una red pública, protegiendo la privacidad y la seguridad de la información.

Hacker ético: Un hacker ético es un profesional de la seguridad informática que busca vulnerabilidades para mejorar la seguridad, no para dañarla.

Ataque de denegación de servicio (DDoS): Un ataque DDoS intenta abrumar un servidor o red con tráfico falso, lo que puede llevar a la inaccesibilidad del sistema.

Hardening: El endurecimiento implica asegurar la configuración de sistemas y aplicaciones para reducir las vulnerabilidades.

Ransomware: El ransomware es un tipo de malware que cifra los datos y exige un rescate para su desbloqueo.

CAPÍTULO II: PLANTEAMIENTO DEL PROBLEMA

2.1. Descripción del Problema

El Hospital César Garayar García de Iquitos se encuentra inmerso en una situación problemática de seguridad informática en el año 2023 que reviste una gravedad crítica. Este problema no solo afecta a nivel local, sino que su alcance se extiende a nivel nacional e internacional. La coyuntura actual se caracteriza por un alarmante incremento de las amenazas cibernéticas, con actores maliciosos empeñados en acceder a información confidencial y datos médicos altamente sensibles. Diversos factores clave agravan esta problemática, en el contexto internacional se ha registrado un notable aumento en los ataques cibernéticos dirigidos a instituciones de salud. En particular, los hospitales se han convertido en objetivos sumamente atractivos para ciberdelincuentes debido a que almacenan información médica personal que puede ser explotada con propósitos ilícitos. Esta tendencia internacional subraya la urgente necesidad de reforzar la seguridad informática en el Hospital César Garayar para preservar la confidencialidad, integridad y disponibilidad de los datos de los pacientes, en el contexto nacional, la infraestructura de salud en el Perú se ha vuelto cada vez más dependiente de la tecnología de la información para gestionar registros médicos, citas, facturación y otros procesos vitales. Esto conlleva un incremento en la cantidad de datos sensibles almacenados en línea, lo que, a su vez, intensifica la exposición a riesgos de seguridad cibernética. Los hospitales deben cumplir con regulaciones nacionales en materia de seguridad de datos, como la Ley de Protección de Datos Personales, lo que añade una capa adicional de responsabilidad en la protección de la información, en el ámbito local, el Hospital César Garayar juega un papel de vital importancia en la atención médica de la población de Iquitos y sus alrededores. La interrupción de los servicios médicos debido a un ataque cibernético podría tener consecuencias devastadoras para la salud de la comunidad. Además, el hospital almacena información de pacientes de la región, lo que lo convierte en un objetivo particularmente atractivo para los ataques cibernéticos locales, los desafíos específicos de esta investigación será la evaluación de la Insuficiencia de recursos y presupuesto para invertir en

medidas de seguridad informática adecuadas, falta de conciencia y capacitación en seguridad informática entre el personal médico y administrativo, necesidad imperante de establecer políticas y procedimientos de seguridad informática efectivos y acordes con las regulaciones locales y nacionales, análisis de vulnerabilidades en la infraestructura de TI y en las aplicaciones utilizadas para la gestión de la atención médica, la constante evolución de las amenazas cibernéticas y la necesidad apremiante de mantenerse al día con las mejores prácticas de seguridad, y como objetivo de esta tesis es investigar y proponer soluciones para fortalecer la seguridad informática en el Hospital César Garayar de Iquitos, considerando el contexto internacional, nacional y local en el año 2023. La presente investigación busca abordar los desafíos específicos mencionados y proponer un marco integral de seguridad informática que proteja la confidencialidad de la información médica, garantice la disponibilidad de servicios de atención médica y cumpla con las regulaciones aplicables.

2.2. Formulación del Problema

2.2.1. Problema General

¿Cuál es el nivel de seguridad informática que tiene el hospital César Garayar García de la ciudad de Iquitos?

2.2.2. Problemas Específicos

1) ¿Cuál es el nivel de seguridad del hardware del hospital César Garayar García de la ciudad de Iquitos?
2) ¿Cuál es el nivel de seguridad de software del hospital César Garayar García de la ciudad de Iquitos?
3) ¿Cuál es el nivel de riesgo de la seguridad informática del hospital César Garayar García de la ciudad de Iquitos?
4) ¿Cuál es el nivel de cumplimiento de políticas de seguridad del hospital César Garayar García de la ciudad de Iquitos?

2.3. Objetivos

2.3.1. Objetivo General

Evaluar el nivel de seguridad informática del hospital César Garayar García de la ciudad de Iquitos

2.3.2. Objetivos Específicos

1) Evaluar el nivel de seguridad del hardware del hospital César Garayar García de la ciudad de Iquitos.
2) Evaluar el nivel de seguridad de software del hospital César Garayar García de la ciudad de Iquitos.
3) Evaluar el nivel de riesgo de la seguridad informática del hospital César Garayar García de la Ciudad de Iquitos.
4) Evaluar el nivel de cumplimiento de políticas de seguridad del hospital César Garayar García de la ciudad de Iquitos.

2.4. Hipótesis

- ✓ **Hipótesis General:**
  - Hipótesis Nula:

    El nivel de seguridad informática del Hospital César Garayar García de la ciudad de Iquitos es bajo.

  - Hipótesis Alternativa:

    El nivel de seguridad informática del Hospital César Garayar García de la ciudad de Iquitos es alto.

2.5. Variables

2.5.1. Identificación de Variables

Variable 1: Nivel de seguridad informática.

2.5.2. Definición Conceptual de las Variables

Variable: Nivel de Seguridad Informática se refiere al grado de protección que tienen los sistemas, redes y datos de una organización contra amenazas cibernéticas y otros riesgos relacionados con la seguridad de la información.

2.5.3. Operacionalización de las Variables

Tabla 1: Operacionalización de Variables

Variables	Dimensiones	Indicadores	Instrumento de Recolección de Datos
Seguridad Informática	Nivel de seguridad del Hardware.	Estado Actual	• Ficha de Observación • Revisión documental • Matriz de Riesgo • Encuesta
	Nivel de seguridad del Software.	Posibles Vulnerabilidades	
	Nivel de Riesgo	Importancia	
		Vulnerabilidad	
		Riesgo	
	Nivel de cumplimiento de políticas de seguridad	% de cumplimiento	

Fuente: Elaboración Propia

CAPÍTULO III: METODOLOGÍA

3.1. Tipo y Diseño de Investigación

- **Tipo de Investigación**

  Investigación de tipo descriptiva y evaluativa. El enfoque descriptivo se utiliza para comprender y describir el estado actual de la seguridad informática en el Hospital César Garayar García en Iquitos en el año 2023. El enfoque evaluativo implica analizar y evaluar el nivel de seguridad informática existente en el hospital. Para llevar a cabo esta investigación, se recopilaron datos, se realizaron evaluaciones de vulnerabilidades y se analizaron las políticas y prácticas de seguridad.

- **Diseño de la Investigación**

  El diseño de la investigación es un estudio de caso, ya que se centra en un caso específico, es decir, el Hospital César Garayar García en Iquitos. En esta investigación se hizo un estudio de caso realizando el análisis detallado y profundo de la entidad, en este caso, el nivel de seguridad informática en el hospital.

3.2. Población y Muestra

Población

La población fue todos los sistemas informáticos, dispositivos, políticas de seguridad y personal relacionado con la seguridad informática en el Hospital César Garayar García en Iquitos en el año 2023.

Muestra

La muestra estará compuesta según se detalla en la siguiente tabla:

Tabla 2: Muestra de la Investigación

Objetivos	Muestra
1.- Evaluación del hardware	1 servidor de Base de Datos
	1 servidor de Aplicaciones
	1 servidor de SIGA
	1 servidor de SIAF
	30 computadoras de Escritorio

	10 computadoras Laptops
	12 impresora Laser
	10 switch de 24 puertos
	8 switch de 12 puertos
	16 cámaras de seguridad
	4 DVR
	4 Router
2.- Evaluación del software	1 sistema Informático de Historias Clínicas
	1 sistema Informático de Caja y Facturación
	1 sistema Informático de Farmacia
	1 sistema Informático SIAF
	1 sistema Informático SIGA
	1 sistema Informático SIS
	1 sistema Informático HIS
3.- Nivel de riesgo	10 activos de Información
4.- Cumplimiento de políticas de seguridad	04 personas del área de informática
	02 personas del área de estadística
	02 personas del área de farmacia
	02 personas del área de caja y recaudación
	02 personas del área de logística
	01 persona del área de tesorería
	02 persona del área de admisión

Fuente: Elaboración Propia

3.3. Técnicas, instrumentos y procedimientos de recolección de datos

- **Técnica de Recolección de Datos:**

  Observación: La técnica de observación se erige como una herramienta fundamental para evaluar la seguridad informática de una organización, permitiendo realizar una evaluación directa de los controles y prácticas de seguridad en ejecución.

  Entrevistas: Realizar entrevistas con el personal de seguridad informática, personal médico y otros empleados del hospital para recopilar información cualitativa sobre políticas de seguridad, prácticas y desafíos de seguridad.

Auditorías de seguridad: Realizar auditorías técnicas para evaluar la seguridad de los sistemas informáticos y redes del hospital. Esto puede incluir pruebas de penetración, análisis de vulnerabilidades y evaluación de configuraciones de seguridad.

- **Instrumento de Recolección de Datos:**

  Ficha de Observación: Se trata de un formato o formulario organizado que se emplea como instrumento para registrar y hacer seguimiento durante una evaluación de seguridad informática.

  Cuestionario: Es un conjunto de preguntas estructuradas diseñadas para recopilar información específica acerca de las prácticas, políticas, procedimientos y controles de seguridad informática en la organización.

  Matriz de riesgo: es una herramienta gráfica y tabular que se utiliza para evaluar y visualizar los riesgos de una determinada situación, proyecto o proceso.

- **Procedimiento de Recolección de Datos:**

  Para recolectar información para realizar el análisis de vulnerabilidades emplearemos la ficha de observación y un cuestionario a los trabajadores de la oficina de informática.

  Para recolectar la información para la evaluación de riesgo emplearemos una matriz de riesgo.

3.4. Procesamiento y análisis de datos.

La Información se procesó en software estadístico SPSS Versión 22, cuyos resultados se clasificaron en cuadros y gráficos estadísticos.

CAPÍTULO IV: RESULTADOS

Resultados de la Variable: Nivel de Seguridad Informática

Dimensión: Evaluación del Hardware

Indicador1: Estado Actual

Tabla 3: Estado Actual de los Activos Hardware del Hospital Iquitos César Garayar García.

N°	Activo de Hardware	Cantidad	Descripción	Estado Actual
1	Servidor de Base de Datos	1	Almacena datos de los sistemas de gestión hospitalaria	Bueno
2	Servidor de Aplicaciones	1	Almacena los sistemas de gestión hospitalaria	Bueno
3	Servidor de SIGA	1	Aloja y gestiona el Sistema de Información de Gestión Administrativa (SIGA) para la administración de recursos y finanzas en la entidad.	Bueno
4	Servidor de SIAF	1	Ejecuta el Sistema Integrado de Administración Financiera (SIAF), permite la gestión y control de los recursos financieros de la organización, incluyendo presupuesto, gastos y recursos.	Bueno
5	Computadoras de Escritorio	30	Estaciones de trabajo utilizadas en diferentes departamentos y oficinas para tareas administrativas, procesamiento de datos y gestión de documentos.	Regular
6	Computadoras Laptops	10	Portátiles utilizados por personal en movimiento o fuera de la oficina para acceder a datos y aplicaciones.	Bueno

7	Impresora Laser	12	Dispositivo de impresión que utiliza tecnología láser para imprimir documentos con alta calidad y velocidad.	Regular
8	Switch de 24 puertos	10	Equipo de red que permite la conexión de múltiples dispositivos en una red local mediante cables Ethernet.	Regular
9	Switch de 12 puertos	8	Similar al switch de 24 puertos, pero con menos puertos para la conexión de dispositivos en una red.	Regular
10	Cámaras de seguridad	16	Dispositivos de videovigilancia utilizados para monitorear áreas de seguridad, control de acceso y vigilancia en el entorno físico del edificio.	Bueno
11	DVR (Grabador de Video)	4	Equipo que graba y almacena las imágenes de video capturadas por las cámaras de seguridad para su posterior revisión y recuperación.	Bueno
12	Router	4	Dispositivo de red que dirige el tráfico de datos entre redes, como la conexión a Internet y redes locales.	Bueno

Fuente: Elaboración propia

La tabla 03 muestra una lista de varios tipos de equipos informáticos que tiene actualmente el Hospital Iquitos César Garayar García, la cantidad de cada tipo de equipo y su estado. El estado se clasifica como "Bueno" en la mayoría de los casos, pero también se indica que el estado de las computadoras de escritorio puede variar entre "Bueno", "Regular" o "Malo" según la situación específica de cada equipo.

Tabla 4: Activos Hardware que necesita el Hospital Iquitos César Garayar García para asegurar la gestión de la información y continuidad de los servicios

N°	Activo de Hardware	Cantidad	Descripción de Aplicación
1	Firewall	1	Un firewall se utiliza para proteger la red del hospital contra amenazas cibernéticas, como intrusiones, malware y ataques de hackers. Ayuda a asegurar que los sistemas y datos médicos estén protegidos y cumplan con las regulaciones de privacidad y seguridad de la información.
2	Switch Core o Administrable	1	El switch Core o administrable se encarga de gestionar y Administrable dirigir el tráfico de datos en la red del hospital, proporciona conectividad confiable y eficiente para los dispositivos y sistemas médicos, garantizando un flujo de datos sin interrupciones en toda la red.
3	Servidor de telefonía IP	1	El servidor de telefonía IP permite la implementación de IP un sistema de telefonía basado en IP en el hospital. Facilita la comunicación interna y externa, la gestión de llamadas de pacientes y la integración con sistemas de registros médicos electrónicos para un mejor servicio.
4	Teléfonos IP	20	Los teléfonos IP se utilizan en el hospital para realizar llamadas de voz sobre IP (VoIP) de alta calidad y videoconferencias. Proporcionan una comunicación eficiente entre el personal médico y con los pacientes.

Fuente: Elaboración propia

La tabla 04 muestra y describe los equipos necesarios y su aplicación de cada tipo de equipo en un entorno hospitalario y cómo contribuye a la infraestructura tecnológica y la comunicación eficiente en un hospital. Cada uno de estos equipos es esencial para garantizar la seguridad y el flujo de datos en un entorno de atención médica en el Hospital Iquitos César Garayar García.

Dimensión: Evaluación del Software

Indicador1: Posibles Vulnerabilidades

Tabla 5: Softwares que tiene el Hospital Iquitos César Garayar García y sus posibles vulneraciones

N°	Software	Posibles Vulneraciones
1	Sistema Informático de Historias Clínicas	1. Acceso no autorizado a registros médicos. 2. Falta de cifrado en la transmisión de datos. 3. Vulnerabilidades en el software utilizado.
2	Sistema Informático de Caja y Facturación	1.Falta de control de acceso a sistemas financieros. 2.Posible fraude en el proceso de facturación. 3. Vulnerabilidades en el software de facturación.
3	Sistema Informático de Farmacia	1.Problemas en la gestión de inventario y stock. 2.Falta de control en la dispensación de medicamentos. 3.Vulnerabilidades en sistemas de pedidos y control.
4	Sistema Informático SIAF	1. Falta de seguridad en la administración Cuentas y fondos. 2. Vulnerabilidades en procesos de autorización. 3. Riesgos en la integridad de datos financieros.
5	Sistema Informático SIGA	1. Acceso no autorizado a datos de recursos humanos y nómina. 2. Problemas de gestión de privilegios. 3. Vulnerabilidades en sistemas de compras y activos.
6	Sistema Informático SIS	1. Riesgos de seguridad en el acceso a registros de pacientes. 2. Posible exposición de datos médicos sensibles. 3. Vulnerabilidades en sistemas de citas y registros.
7	Sistema Informático HIS	1. Problemas en la integridad y disponibilidad de registros médicos y operacionales. 2. Acceso no autorizado a sistemas críticos. 3. Vulnerabilidades en sistemas de admisión y alta.

Fuente: Elaboración propia

La tabla 05 muestra las posibles vulnerabilidades que cada uno de los sistemas informáticos mencionados esta evaluación se realizó evaluando los sistemas desde diferentes ángulos, incluyendo su arquitectura, configuración, políticas de seguridad y prácticas operativas. Las vulnerabilidades pueden incluyen configuraciones incorrectas, falta de actualizaciones de seguridad, debilidades en el software, falta de control de acceso, entre otros.

Dimensión: Nivel de riesgo

Indicadores: Importancia, Vulnerabilidad, Riesgo

Tabla 6: Matriz de Riesgo de Activos de Información del Hospital César Garayar García de la ciudad de Iquitos

Activos de Información	**Importancia (Alta, Media, Baja)**	**Vulnerabilidad (Alta, Media, Baja)**	**Riesgo (Crítico, Alto, Medio, Bajo)**
Historias clínicas de Pacientes	Alta	Alta	Crítico
Datos de Pacientes	Alta	Alta	Crítico
Información Financiera del Hospital	Alta	Media	Alto
Sistemas de Información Médica	Alta	Media	Alto
Documentación de Políticas y Normativas	Alta	Baja	Medio
Datos de Empleados del Hospital	Media	Alta	Alto
Registros de Pacientes Internados	Alta	Media	Alto
Información de Proveedores	Media	Baja	Medio
Datos de Laboratorios Médicos	Alta	Media	Alto
Sistema de Reservas de Citas	Media	Baja	Medio

Fuente: Elaboración propia

En la tabla 06 se muestra la matriz de riesgo de activos para la seguridad informática del Hospital Iquitos César Garayar García, En esta tabla, se enlistan los activos de información crítica, se evalúan en función de su importancia y vulnerabilidad, y se asigna un nivel de riesgo.

Cada activo se coloca en una de las siguientes categorías de riesgo:

- Crítico: Activos de alta importancia y alta vulnerabilidad, que son fundamentales y deben protegerse con la máxima prioridad.
- Alto: Activos de alta importancia y vulnerabilidad media o alta, que requieren una gestión de riesgos significativa.
- Medio: Activos de importancia media y vulnerabilidad media, que requieren medidas de seguridad moderadas.
- Bajo: Activos de importancia baja y vulnerabilidad baja o media, que requieren supervisión, pero pueden ser de menor prioridad en la gestión de riesgos.

Esta matriz de riesgo de activos ayuda al Hospital Iquitos César Garayar García a identificar y priorizar los activos críticos que requieren una atención especial en términos de seguridad informática y a tomar medidas adecuadas para protegerlos.

Dimensión: Cumplimiento de políticas de seguridad

Indicador 1: Políticas Implementadas

Tabla 7: Políticas de seguridad informática implementadas en el Hospital César Garayar García de la ciudad de Iquitos

N°	Política de Seguridad Informática	Estado de implementación	Detalle
1	Política de Acceso y Autenticación	Parcialmente implementada	Se requiere mejorar la autenticación y el control de accesos.
2	Política de Seguridad Física	Parcialmente implementada	Se han implementado medidas de seguridad física, pero no se ha incluido el control de acceso.
3	Política de Protección de Datos de Salud (HIPAA, RGPD, etc.)	Parcialmente implementada	La protección de datos de salud está en proceso de cumplimiento
4	Política de Gestión de Incidentes de Seguridad	No implementada	No se ha iniciado la implementación de procedimientos de gestión de incidentes

5	Política de Copias de Seguridad y Recuperación (Backup)	Parcialmente implementada	Se realiza copias de seguridad en el mismo disco duro de los servidores, pero no se crea una biblioteca de backup de manera externa
6	Política de Navegación Segura en la Web y Correo Electrónico	No Implementada	No se cuenta con un corta fuegos
7	Política de Actualización de Software y Parches	No implementada	No se cuenta con un servidor de memoria cache para las descargas y almacenamiento de las actualizaciones
8	Política de Concienciación en Seguridad Informática	No implementada	No se promueven capacitaciones al personal sobre concientización
9	Política de Acceso a redes Inalámbricas (Wi-Fi)	Parcialmente implementada	Solo existe un nivel mínimo de seguridad para acceder a los router
10	Política de Privacidad de Datos	Parcialmente implementada	Solo esta implementada en los servidores de los sistemas que proporciona el estado

Fuente: Elaboración propia

En la tabla 07 se muestra el estado de implementación de varias políticas de seguridad informática en el hospital. Puede haber políticas implementadas en diferentes grados y, en algunos casos, serán necesarias mejoras para lograr un nivel óptimo de seguridad. La unidad de informática del hospital debería trabajar continuamente en la implementación y mejora de estas políticas para garantizar la protección de sus activos y la privacidad de los datos.

Prueba de Hipótesis

De acuerdo a los resultados de las dimensiones e indicadores de nuestra investigación se pudo determinar que el nivel de seguridad informática del Hospital César Garayar García de la ciudad de Iquitos es baja, por lo tanto, aceptamos la hipótesis nula y rechazamos la hipótesis alternativa.

CAPÍTULO V: DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

Discusiones

Discusión 1: Evaluación del Hardware, El primer conjunto de datos proporcionado en la tabla N°03 muestra el estado actual de los activos de hardware del Hospital Iquitos César Garayar García. La discusión se centra en la evaluación de la infraestructura de hardware utilizada en el hospital. En general, la mayoría de los activos de hardware, como servidores, computadoras portátiles y cámaras de seguridad, se encuentran en un estado "bueno". Sin embargo, se observa que algunas computadoras de escritorio, impresoras láser y switches de red se clasifican como "regulares".

Discusión 2: Necesidades de Hardware, La tabla N°04 destaca los activos de hardware necesarios para asegurar la gestión de la información y la continuidad de los servicios en el Hospital Iquitos César Garayar. Estos activos son esenciales para garantizar la seguridad de los datos y el funcionamiento eficiente de las operaciones del hospital. La discusión aquí se centra en la importancia de contar con un firewall para proteger la red contra amenazas cibernéticas, un switch Core para gestionar el tráfico de datos, un servidor de telefonía IP para mejorar la comunicación y teléfonos IP para la eficiente comunicación interna y externa.

Discusión 3: Posibles Vulnerabilidades del Software, La tabla N°05 presenta posibles vulnerabilidades en los sistemas informáticos utilizados en el hospital. Cada sistema se evalúa en términos de las amenazas potenciales, como el acceso no autorizado a registros médicos o vulnerabilidades en el software. Esta discusión resalta la importancia de identificar y mitigar estas vulnerabilidades para proteger los datos y garantizar la seguridad de la información médica y financiera del hospital.

Discusión 4: Matriz de Riesgo de Activos de Información, La tabla N°06 muestra una matriz de riesgo que evalúa la importancia, vulnerabilidad y riesgo de los activos de información en el hospital. La discusión se centra en la categorización de activos en términos de su nivel de riesgo, desde "crítico" hasta "bajo". Esto destaca la importancia de priorizar la protección de activos críticos, como las historias clínicas de pacientes y los datos financieros del hospital, y la necesidad de implementar medidas de seguridad adecuadas para mitigar los riesgos.

Conclusiones

1) Se concluye que la evaluación del hardware en el Hospital Iquitos César Garayar García muestra que la mayoría de los activos de hardware, incluidos servidores, computadoras portátiles y cámaras de seguridad, se encuentran en un estado "bueno". Sin embargo, es importante abordar el estado "regular" de algunas computadoras de escritorio, impresoras láser y switches de red para garantizar un entorno informático más robusto y seguro.
2) Se concluye que la identificación de activos de hardware necesarios destaca la importancia de inversiones en tecnología para fortalecer la seguridad y la eficiencia operativa en el hospital. La implementación de un firewall, un switch Core, un servidor de telefonía IP y teléfonos IP mejorará significativamente la infraestructura tecnológica del hospital y su capacidad para brindar atención médica de calidad.
3) Se concluye que la identificación de posibles vulnerabilidades en los sistemas informáticos es un paso crucial para garantizar la seguridad de la información médica y financiera. Las amenazas potenciales, como el acceso no autorizado y las vulnerabilidades en el software, deben abordarse mediante la implementación de medidas de seguridad y la actualización regular de los sistemas para reducir los riesgos.
4) Se concluye que la matriz de riesgo de activos de información resalta la importancia de priorizar la protección de activos críticos, como las historias clínicas de pacientes y los datos financieros del hospital. La clasificación de activos en categorías de riesgo "crítico" y "alto" subraya la necesidad de implementar medidas de seguridad efectivas y estratégicas para mitigar los riesgos y garantizar la integridad y confidencialidad de la información en el entorno hospitalario.

Recomendaciones

1) Se recomienda implementar un programa de mantenimiento preventivo y correctivo para los equipos de hardware clasificados como "regulares" en la evaluación. Esto ayudará a prolongar la vida útil de los activos, mejorar su rendimiento y reducir el riesgo de fallos inesperados. El mantenimiento debe incluir la actualización de software, limpieza y reparación de hardware según sea necesario.
2) Dado que se identificaron posibles vulnerabilidades en los sistemas informáticos, se recomienda implementar medidas de seguridad adicionales, como la aplicación de actualizaciones de software y parches de seguridad. También es importante llevar a cabo auditorías de seguridad regulares para identificar y corregir vulnerabilidades antes de que puedan ser explotadas por amenazas cibernéticas.
3) Se recomienda adquirir los activos de hardware necesarios, como un firewall, un switch Core, un servidor de telefonía IP y teléfonos IP. Estos equipos son fundamentales para mejorar la seguridad de la red y la comunicación en el hospital. La inversión en tecnología apropiada contribuirá a la eficiencia operativa y la protección de datos sensibles.
4) Las políticas de seguridad informática parcialmente implementadas requieren una atención inmediata. Se recomienda desarrollar e implementar políticas de seguridad de acceso y autenticación, seguridad física, protección de datos de salud y gestión de incidentes de seguridad. Estas políticas son esenciales para garantizar un entorno seguro y cumplir con las regulaciones de seguridad de la información en la atención médica.
5) La matriz de riesgo resalta la importancia de priorizar la seguridad de activos críticos, como las historias clínicas de pacientes y los datos financieros. Se recomienda asignar recursos y esfuerzos adicionales para proteger y respaldar estos activos. Esto puede incluir la implementación de medidas de seguridad avanzadas, copias de seguridad regulares y controles de acceso estrictos. La seguridad de estos activos debe ser una prioridad máxima en la estrategia de seguridad informática del hospital.

Referencias Bibliográficas:

- SALAZAR-CHALCO, Juan Pablo; CAMPOVERDE-MOLINA, Milton. Detección de vulnerabilidades informáticas en estaciones de trabajo: Caso de estudio Hospital de Especialidades José Carrasco Arteaga. Polo del Conocimiento, 2022, vol. 7, no 4, p. 446-465.
- ARISMENDI RAMÍREZ, Jonathan, et al. Análisis de riesgos y diagnóstico de la seguridad de la información de la ESE Hospital Santa Mónica, bajo los parámetros de la seguridad informática. 2018.
- CORDERO MORENO, José Leonardo, et al. Análisis de riesgos y recomendaciones de seguridad de la información del Hospital ESE San Bartolomé de Capitanejo, Santander. 2016.
- MALAGÓN LARA, Juan Carlos, et al. Análisis de las técnicas de ingeniería social que amenazan la seguridad informática de usuarios de entidades financieras.
- CUTIN ZAPATA, Alipio. Análisis y diseño de un plan de seguridad informática en la municipalidad distrital de Canchaque–Piura; 2020.
- CHAVEZ BARDALES, Eduardo Adriam Benyamin; DAVILA VALERA, Willy Esteban. EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA DEL HOSPITAL III IQUITOS DE ESSALUD LORETO-2022. 2022.
- López M y Lobato F. (2006) Operaciones de ventas, Editorial Paraninfo, Madrid España.
- Lujan S. (2002) Programación de aplicaciones web: historia, principios básicos y clientes web, Editorial.
- Martinez J. y Rojas F. (2016) Comercio electrónico, Editorial Paraninfo 1° Edición, Madrid España.
- Moliner F. (2005) Grupo A y B de Informática Bloque Especifico Volumen II, Mad, Barcelona, España

Anexo 1. Matriz de consistencia.

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	DIMENSIÓN	INDICADORES	METODOLOGIA
Problema General **¿Cuál es el nivel de seguridad informática que tiene el Hospital César Garayar García de la ciudad de Iquitos?** **Problemas Específicos** ¿Cuál es el nivel de seguridad del hardware del Hospital César Garayar García de la ciudad de Iquitos? ¿Cuál es el nivel de seguridad de software del Hospital César Garayar García de la ciudad de Iquitos?	General Evaluar el nivel de seguridad informática del Hospital César Garayar García de la ciudad de Iquitos Específicos Evaluar el nivel de seguridad del hardware del Hospital César Garayar García de la ciudad de Iquitos. Evaluar el nivel de seguridad de software del Hospital César Garayar	**Hipótesis General:** Hipótesis Nula: El nivel de seguridad informática del Hospital César Garayar García de la ciudad de Iquitos es bajo. Hipótesis Alternativa: El nivel de seguridad informática del Hospital César Garayar García de la ciudad de Iquitos es alto.	Variable Nivel de Seguridad Informática	Nivel de seguridad del Hardware. Nivel de seguridad del Software. Nivel de Riesgo	Estado Actual Posibles Vulnerabilidades Importancia Vulnerabilidad Riesgo	Tipo de Investigación Investigación de tipo descriptiva y evaluativa. El diseño de la investigación es un estudio de caso Población y Muestra Población la población fue todos los sistemas informáticos, dispositivos, políticas de seguridad y personal relacionado con la seguridad informática en el Hospital César Garayar García en Iquitos en el año 2023. Técnica de Recolección de Datos: La Observación La encuesta Instrumento de Recolección de Datos:

¿Cuál es el nivel de riesgo de la seguridad informática del Hospital César Garayar García de la ciudad de Iquitos? ¿Cuál es el nivel de cumplimiento de políticas de seguridad del Hospital César Garayar García de la ciudad de Iquitos?	García de la ciudad de Iquitos. Evaluar el nivel de riesgo de la seguridad informática del Hospital César Garayar García de la Ciudad de Iquitos. Evaluar el nivel de cumplimiento de políticas de seguridad del Hospital César Garayar García de la ciudad de Iquitos.			Nivel de cumplimiento de políticas de seguridad	% Cumplimiento	Ficha de Observación Cuestionario Procedimiento de Recolección de Datos: La Información será procesada en software estadístico, cuyos resultados serán clasificados en cuadros y gráficos estadísticos.

Anexo 2. Carta de Autorización para la evaluación del Nivel de Seguridad Informática del Hospital Iquitos “César Garayar García”

CARTA DE AUTORIZACIÓN PARA LA EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA

El que suscribe, **Ing. DICK BRAND REATEGUI MENDOZA**, Jefe de la Unidad de Estadística e Informática del Hospital Apoyo Iquitos “César Garayar García”, autoriza a los Bachilleres **JUAN ARTURO RUIZ CÁCERES y JORGE JUNIOR SÁNCHEZ RIOS**, para realizar una evaluación del nivel y estado situacional de la seguridad informática del hospital, como parte del desarrollo de sus tesis titulada **“ANÁLISIS DEL NIVEL DE SEGURIDAD INFORMÁTICA DEL HOSPITAL CÉSAR GARAYAR GARCÍA IQUITOS-2023”**, en la facultad de Ciencias e Ingeniería, programa académico de Ingeniería de Sistemas de Información.

Iquitos, 22 de agosto del 2023

Atentamente,

GOBIERNO REGIONAL DE LORETO
GERENCIA REGIONAL DE SALUD
HOSPITAL “CESAR GARAYAR GARCIA”
ING. DICK BRAND MENDOZA REATEGUI
CIP:142373
JEFE DE LA UNIDAD DE ESTADISTICA E INFORMATICA